

Opis przedmiotu zamówienia

Dostarczenie systemu informatycznego zawierającego zbiór informacji o interakcjach lekowych w systemach Centrum e-Zdrowia

1. Wprowadzenie.....	3
1.1. Termin realizacji zamówienia	3
1.2. Przedmiot zamówienia.....	3
2. Słownik pojęć:.....	4
3. Cel systemu	8
4. Wymagania funkcjonalne	8
4.1. Zakres funkcjonalny	8
5. Wymagania pozafunkcjonalne.....	12
5.1 Wymagania w zakresie architektury	12
5.2 Obsługiwane formaty danych i protokoły komunikacyjne	14
5.3 Bezpieczeństwo i kontrola danych	15
5.4 Wymagania w zakresie wydajności i skalowalności.....	18
5.5 Wymagania w zakresie infrastruktury.....	18
5.6 Wymagania dotyczące licencji i praw autorskich	20
5.7 Wymagania w zakresie użyteczności	20
5.8 Wymagania dotyczące Dokumentacji.....	21
5.9 Rejestrowanie zdarzeń i logi Systemowe	21
6. Dostarczane elementy	23
6.1 System.....	23
6.2 Model świadczenia usługi.....	23
6.3 Licencje i Kod Źródłowy.....	24
6.4 Usługa Serwisowa.....	24

6.5 Gwarancja	24
6.6 Instruktaż stanowiskowy	25
7. Obowiązki Wykonawcy	27
7.1 Wersjonowanie Systemu i planowane przerwy serwisowe	27
7.2 Testy wydajnościowe	28
7.2.1 Rodzaje testów:	29
7.2.2. Środowisko testowe	29
7.2.3. Cykliczność testów	30
7.3 Testy bezpieczeństwa	30
7.4 Testy integracyjne	31
7.5 Weryfikacja jakości Kodu Źródłowego	31
7.6 Usługi Gwarancyjne i Serwisowe	32
7.7 Usługi Rozwojowe	32
7.8 Ogólny Harmonogram Wdrożenia Systemu	32
7.9 Dokumentacja	32
7.9.1 Wymagania ogólne	32
7.9.2 Dokumentacja Administratora Systemu	33
7.9.3 Dokumentacja Użytkownika Systemu	33

1. Wprowadzenie

1.1. Termin realizacji zamówienia

Maksymalnie 60 dni od daty zawarcia Umowy, lecz nie później niż do 31.05.2026 r.

1.2. Przedmiot zamówienia

Przedmiotem Umowy/zamówienia jest dostarczenie:

w ramach zamówienia podstawowego:

- 1) Systemu w modelu 1 lub 2 opisany w punkcie 6.2
- 2) Systemu do analizy i porównania interakcji lekowych, umożliwiające ocenę bezpieczeństwa jednoczesnego stosowania wielu substancji leczniczych u pacjentów, wraz z bazą interakcji lekowych
- 3) dostarczenie bazy leków zarejestrowanych na terytorium RP wraz z aktualizacjami przez okres 60 miesięcy.
- 4) zapewnienie przez Wykonawcę Usług Gwarancyjnych zdefiniowanych w załączniku nr 1 przez okres 60 miesięcy od dnia odbioru przez Zamawiającego Wdrożenia Systemu,
- 5)

w ramach zamówienia opcjonalnego rozdzielnie:

- 6) świadczenie przez Wykonawcę Usług Rozwojowych określonych w załączniku nr 3
- 7) zapewnienie przez Wykonawcę Usług Serwisowych zdefiniowanych w załączniku nr 1 przez okres 60 miesięcy od dnia odbioru przez Zamawiającego Wdrożenia Systemu,
- 8) dostarczenie bazy refundowanych wyrobów medycznych i środków spożywczych specjalnego przeznaczenia żywieniowego oraz innych dostępnych w aptekach produktów (suplementów diety, kosmetyków itp.) wraz z aktualizacjami przez okres 60 miesięcy.
- 9) dostarczenie bazy interakcji leków z innymi substancjami czynnymi, żywnością i/lub suplementami diety, itp. wraz z aktualizacjami przez okres 60 miesięcy.
- 10) dostarczenie bazy wskazań, przeciwwskazań i ostrzeżeń dla poszczególnych produktów leczniczych oraz działań niepożądanych. wraz z aktualizacjami przez okres 60 miesięcy.

2. Słownik pojęć:

Pojęcie	Definicja/Opis
Zamawiający	Centrum e-Zdrowia
CeZ	Centrum e-Zdrowia
Wykonawca	Podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego
Gwarancja i Serwis	Zobowiązanie Wykonawcy, udzielone Zamawiającemu na warunkach określonych w Umowie, obejmujące Wdrożenie, System oraz wszystkie Rezultaty, zgodnie z którym Wykonawca zapewnia, że w okresie gwarancyjnym będą one zgodne z postanowieniami Umowy, OPZ oraz Ofertą Wykonawcy oraz wolne od Wad, w tym Wad Prawnych.
Usługa Serwisowa	Usługa obejmująca wszelkie czynności mające na celu zapewnienie prawidłowego, bezpiecznego i wydajnego działania Systemu. Usługa obejmuje w szczególności: - proaktywne monitorowanie, analizę logów, rekomendowanie rozwiązań oraz integrację z narzędziami monitoringu i bezpieczeństwa Zamawiającego, - działania zapobiegające Incyidentom, w tym usuwania podatności, dostarczanie narzędzi do wykonywania kopii zapasowych oraz rekomendowanie usprawnień zwiększających bezpieczeństwo i skalowalność, - usuwanie Wad i obsługę Incyidentów zgodnie z parametrami SLA, w tym analizę zgłoszeń, przygotowanie i wdrażanie Poprawek oraz przywracanie prawidłowego działania Systemu, - bieżące wsparcie techniczne Zamawiającego, w tym dostępność ekspertów, udostępnianie kanałów zgłoszeń (24/7), konsultacje, wsparcie w tworzeniu raportów, monitorowaniu incyidentów bezpieczeństwa, a także przy aktualizacjach i konfiguracji środowisk. Szczegółowy zakres Usługi Serwisowej opisuje Załącznik nr 1 Usługa Serwisowa. Szczegółowy zakres Usługi Serwisowej opisuje Załącznik nr 1 Usługa Serwisowa
Usługa Rozwojowa lub Usługa Rozwoju	Usługa obejmująca modyfikowanie, konfigurację lub rozszerzanie funkcjonalności Systemu, a także tworzenie lub aktualizację powiązanych elementów, takich jak Dokumentacja, interfejsy, moduły, bazy danych, algorytmy czy integracje z innymi systemami informatycznymi. Usługa Rozwojowa ma na celu dostarczenie nowych lub ulepszonych funkcjonalności Systemu.
Dokumentacja	Wszelka dokumentacja i informacje dotyczące Systemu, jak również poszczególnych rezultatów pracy Wykonawcy, zarówno w postaci

	elektronicznej jak i papierowej, niezależnie od nośnika, na którym zostały utrwalone, która powstanie w ramach realizacji Umowy lub do dostarczenia której zobowiązany jest Wykonawca, w szczególności dokumentacja projektowa, powykonawcza, techniczna, środowiskowa, wytwórcza, dokumentacja dotycząca Systemu, dokumentacja niezbędna do przeprowadzenia i aktualizacji DPIA
API	Interfejs programowania aplikacji (z ang. Application Programming Interface) Jest to ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych. Elementem API jest dokumentacja techniczna umożliwiająca jego wykorzystanie przez zewnętrzne systemy.
System	System informatyczny – rozwiązanie obejmujące silnik analizy interakcji lekowych wraz z bazą wiedzy, udostępniane w jednym z dwóch modeli dostawy: • Model A – dostęp do usługi API (SaaS), • Model B – instalacja rozwiązania w infrastrukturze Zamawiającego (on-premise). W obu wariantach System obejmuje warstwę usługową (API). W wariantcie on-premise System może obejmować dodatkowe komponenty techniczne niezbędne do instalacji, konfiguracji i administracji.
Wdrożenie	Etap cyklu życia Systemu, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego oraz testowaniu i uruchomieniu narzędzia. Podstawowe etapy procesu wdrożenia: 1) Przygotowanie dokumentacji, 2) Przygotowanie i skonfigurowanie infrastruktury technicznej, 3) Zainstalowanie i skonfigurowanie narzędzia eksploatacji, 4) Testowanie, 5) Uruchomienie produkcyjne. 6) Szkolenia
Dokumentacja powdrożeniowa	Dokumentacja przygotowana przez Wykonawcę, w związku z realizacją Umowy, specyfikacja opisująca funkcje wdrożonego systemu. W szczególności, w zakresie użytkowania systemu oraz administrowania nim, w języku polskim.
Instruktaż stanowiskowy	Szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora.

Szczegółowy Harmonogram Realizacji	Szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w uzgodnieniu z Zamawiającym
Protokół odbioru	1) Etapu – Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego stanowi potwierdzenie wykonania prac przewidzianych w ramach Etapów określonych w Umowie i uszczegółowionych w Dokumentacji Analizy Przedwdrożeniowej. 2) Końcowy – Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego, stanowi potwierdzenie wykonania i odbioru Przedmiotu Zamówienia. 3) Rozbieżności – Protokół, w którym Zamawiający wskazuje zastrzeżenia co do zakresu i jakości wykonanych prac, które uniemożliwiają dokonanie odbioru wykonanych prac
Dzień Roboczy	Dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy u Zamawiającego w godzinach 6-22
HelpDesk (HD)	Narzędzie posiadające interfejs WWW służące do rejestracji zgłoszeń (potencjalnych problemów, usterek) oraz kontroli ich cyklu życia (tzw. Issue Tracking System lub Defect Tracking System). System udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia oraz w okresie jego gwarancji.
Zgłoszenie Serwisowe (Zgłoszenie)	Zgłoszenie – zaewidencjonowane w HD zdarzenie dotyczące Oprogramowania Aplikacyjnego.
Czas reakcji	Czas reakcji serwisu liczony jest w godzinach od chwili zaewidencjonowania zgłoszenia serwisowego w narzędziu HelpDesk do momentu przyjęcia lub odebrania zgłoszenia tj. nadania mu statusu „nowe”.
Błąd systemu	Działanie powtarzalne, pojawiające się za każdym razem w tym samym miejscu w aplikacji i prowadzące za każdym razem do otrzymywania błędnych wyników jej działania. Podatność bezpieczeństwa, która stwarza ryzyko wykorzystania przez atakującego do uzyskania nieautoryzowanego dostępu, zakłócenia działania systemu, kradzieży danych lub przejęcia kontroli nad systemem bądź infrastrukturą IT. Z definicji wyłącza się błędy powodowane przez następujące okoliczności: 1) zastosowanie systemu w sposób niezgodny z przeznaczeniem, 2) zastosowanie systemu w sposób niezgodny z Dokumentacją, 3) błędne wprowadzenie przez Użytkownika danych, 4) wadliwe zasilanie, awaria klimatyzacji lub urządzeń utrzymujących wilgotność powietrza, a także awarii nośników danych po stronie Zamawiającego, 5) działanie wirusa komputerowego po stronie Zamawiającego, 6) wdrożenie systemu wykonanego w sposób wadliwy, z wyłączeniem sytuacji, w której to było wykonywane przez Wykonawcę,

	7) niewłaściwa parametryzacja systemu oraz bazy danych, z którym ten współpracuje, z wyłączeniem sytuacji, w której to było wykonane przez Wykonawcę, 8) użytkowanie systemu ze złamaniem obwarowań licencyjnych nałożonych na Zamawiającego postanowieniami umowy licencyjnej.
Awaria (błąd krytyczny)	Oznacza sytuację, w której nie jest możliwe prawidłowe używanie systemu, z powodu m.in. uszkodzenia lub utraty kodu programu, struktur danych lub zawartości bazy danych. Podatność krytyczna, potencjalnie możliwa do wykorzystania przez atakującego nie posiadającego uprawnień uprzywilejowanych.
Konsultacja	Usługa świadczona przez Wykonawcę polegająca na udzielaniu Zamawiającemu wyjaśnień w kwestiach dotyczących systemu.
Usterka Programistyczna	Błąd systemu, mimo identyfikacji którego system nadal funkcjonuje, lecz jej eksploatacja jest uciążliwa, skomplikowana lub spowolniona, a usunięcie Błędu wymaga wykonania prac programistycznych przez Producenta.
Uaktualnienie (update)	Wszelkie powszechnie udostępniane przez Producenta modyfikacje Oprogramowania powodujące usunięcie wykrytych Błędów w ramach przedmiotu zamówienia systemu
Rozwinięcie (upgrade)	Wszelkie powszechnie udostępniane przez Producenta nowe wersje lub inne niż Uaktualnienie (update) modyfikacje systemu, zmieniające dotychczasową funkcjonalność systemu
Obejście	udostępnione Zamawiającemu doraźne rozwiązanie mające na celu zminimalizowanie skutków Błędu systemu, zanim zostanie całkowicie usunięty. Zastosowanie obejścia jest zależne od woli Wykonawcy
Czas Naprawy	czas pomiędzy Zgłoszeniem Serwisowym a usunięciem/rozwiązaniem przyczyny jego zgłoszenia
Użytkownik	osoba korzystająca z Aplikacji
Internetowe Konto Pacjenta (IKP)	Bezpłatna aplikacja Ministerstwa Zdrowia, która zapewnia bezpieczny dostęp do informacji o zdrowiu, e-dokumentacji (e-recepty, e-skierowania, wyniki badań) oraz umożliwia zarządzanie sprawami medycznymi online (np. wybór lekarza, upoważnianie bliskich).
mojeIKP	aplikacja mobilna umożliwiająca dostęp do części funkcjonalności Internetowego Konta Pacjenta
Gabinet	aplikacja Centrum e-Zdrowia (CeZ) dla personelu medycznego i podmiotów leczniczych do obsługi procesów medycznych oraz wymiany danych w ramach centralnych usług e-zdrowia.
ATC	Anatomiczno-Terapeutyczny System Klasyfikacji Chemicznej

GTIN	Globalny Numer Jednostki Handlowej – w przypadku produktów leczniczych zarejestrowanych na terenie RP GTIN-14, czyli 14-cyfrowy kod jednoznacznie identyfikujący lek
RPL	Rejestr Produktów Leczniczych
ChPL	Charakterystyka Produktu Leczniczego
RPL	Rejestr Produktów Leczniczych
LSF	Lista Surowców Farmaceutycznych
DDD	Dobowa Dawka Leku ustalona przez WHO
NFC	Trzyliterowy kod postaci leku opracowany przez Ephmra

3. Cel systemu

Udostępnienie systemom CeZ poprzez interfejs API dostępu do bazy interakcji lekowych w celu zwiększenia bezpieczeństwa farmakoterapii, ograniczenia ryzyka działań niepożądanych oraz wsparcia procesu podejmowania decyzji klinicznych przez personel medyczny.

Interfejs API stanowi warstwę usługową Systemu, która przetwarza dane lekowe i zwraca wystandaryzowane odpowiedzi zgodnie z wymaganiami niniejszego przedmiotu zamówienia

4. Wymagania funkcjonalne

4.1. Zakres funkcjonalny

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany
WF.01	API przyjmuje jako dane wejściowe listę leków obejmującą co najmniej 2 i co najwyżej do 10 pozycji w jednym wywołaniu API i zwraca informacje o potencjalnych interakcjach. Dane wejściowe: - kody GTIN - nazwie handlowej - nazwie międzynarodowej substancji czynnej (INN) - kodzie ATC - danych z RPL/URPL Dane wyjściowe:	Wymagany

	• listę wszystkich interakcji • siła interakcji (w skali co najmniej 3-stopniowej) • prawdopodobieństwo kliniczne (w skali co najmniej 3-stopniowej) • opis mechanizmu interakcji, w tym interakcje pośrednie (np. potęgowanie działania przez grupę lekową) • grupowanie interakcji wg ryzyka • skutki kliniczne • rekomendacje lub ostrzeżenia dla lekarza • źródło i data aktualizacji danych	
WF.02	System musi wskazywać interakcje dla substancji czynnych wszystkich leków zarejestrowanych w RPL i LSF.	Wymagany
WF.03	Baza interakcji powinna obejmować wszystkie produkty lecznicze zarejestrowane/dostępne na terenie RP od 01.01.2019 r. oraz dane dotyczące interakcji co najmniej na podstawie informacji zawartych w ChPL.	Wymagany
WF.04	Zakres bazy leków - podstawowy: • aktualna baza leków dopuszczonych do obrotu w Polsce; • kody i identyfikatory (GTIN, ATC, typ produktu (lek, suplement diety, wyrób medyczny itd.), kategoria dostępności (OTC, Rpw, itd.), status rejestracyjny (dopuszczony do obrotu, skrócone pozwolenie itp., wraz z danymi historycznymi od 1.01.2019 r.); • podstawowe dane leku (nazwa handlowa, nazwa międzynarodowa – INN/substancje czynne podane jednolicie, dawka podana w sposób ustrukturyzowany dla każdej INN leku, wielkość opakowania opisana jednolicie w ramach postaci leku, postać leku podana w sposób ujednolicony, droga podania, DDD, warunki przechowywania) • producent/podmiot odpowiedzialny/dystrybutor (jeśli dostępne)	Wymagany
WF.05	Zakres bazy leków - dodatkowe dane o leku: • kod NFC, wykazy farmakopealne/kategoria narkotyczna/psychotropowa, • możliwość podziału tabletki • dane o dawkowaniu • wskazania (ICD-10),	Opcjonalne

	• przeciwwskazania (ICD-10) • ostrzeżenia (stosowanie z alkoholem, wpływ na OUN itp.)	
WF.06	Pobieranie szczegółowych opisów interakcji API zwraca pełny opis interakcji zawierający: • mechanizm farmakokinetyczny / farmakodynamiczny, • potencjalne działania niepożądane wynikające z interakcji, • możliwe konsekwencje kliniczne, • alternatywne opcje terapeutyczne, • źródła (np. ChPL, literatura kliniczna).	Wymagany
WF.07	Wersjonowanie i walidacja baz danych API udostępnia informację o: • wersji bazy leków • wersji bazy interakcji, • dacie ostatniej aktualizacji, • statusie zgodności z bazą centralną, • sposobie synchronizacji (np. cykliczne pobieranie metadanych).	Wymagany
WF.08	API zwraca informację o nierozpoznanym leku lub substancji	Wymagany
WF.09	API musi: • zgłaszać błąd w przypadku niejednoznacznych wpisów/zapytań; (np. nazwa pasuje do wielu produktów), • zwrócić informację, które leki nie zostały rozpoznane, • sygnalizować, jeśli baza wiedzy nie posiada danych o danej interakcji.	Wymagany
WF.10	Uwzględnianie drogi podania i postaci leku: • Automatyczne różnicowanie ciężkości interakcji w zależności od drogi podania (np. doustna, miejscowa, dożylna); • Korekta oceny ryzyka, jeśli zmiana drogi podania modyfikuje znaczenie kliniczne interakcji.	Wymagany
WF.11	Rekomendacje kliniczne przy istotnych interakcjach: • propozycje bezpieczniejszych alternatyw; • rekomendacje modyfikacji dawkowania lub odstępu czasowego; • wskazanie potrzeby monitoringu parametrów (np. stężenie leku).	Opcjonalne

WF.12	API musi umożliwiać: • filtrowanie po poziomie ciężkości • sortowanie wyników (np. najcięższe najpierw), • konfigurację, czy zwracać brak interakcji, • wybór poziomu szczegółowości: krótkie podsumowanie / pełny opis kliniczny.	Wymagany
WF.13	API musi zwracać aktualnie używaną wersję bazy wiedzy,	Wymagany
WF.14	API musi umożliwiać żądanie przetwarzania wg wskazanej wersji	Wymagany
WF.15	Wszystkie funkcjonalności systemu muszą być dostarczone w języku polskim.	Wymagany
WF.16	Aktualizacje: • aktualizacja bazy interakcji leków co najmniej co 14 dni; • informacja o zmianach w wersji (changelog); • stabilność identyfikatorów leków. • utrzymywanie informacji o lekach niedostępnych w obrocie (znacznik)	Wymagany
WF.17	System powinien zapewniać automatyczną aktualizację bazy interakcji oraz leków w celu utrzymania aktualności danych wykorzystywanych w systemie bez konieczności ręcznej interwencji administratora	Wymagany
WF.18	Transparentność zmian: • pełny rejestr aktualizacji; • oznaczenie daty publikacji każdej informacji o interakcji.	Wymagany
WF.19	System alertów — zarządzanie przeciążeniem alertami: • Priorytetyzacja alertów (co najmniej 3-stopniowa); • Streszczenie alertu z możliwością rozwinięcia szczegółów; • Scalanie pokrewnych lub powtarzających się ostrzeżeń; • Możliwość filtrowania alertów wg ważności.	Wymagany
WF.20	Generowanie podsumowania analizy interakcji zawierającego: • klasyfikację i opis mechanizmów; • poziom wiarygodności; • rekomendacje kliniczne; • źródła i datę aktualizacji bazy;	Wymagany

	Eksport raportu do PDF.	
WF.21	Generowanie pełnej macierzy interakcji N×N.	Wymagany
WF.22	W ramach systemu dostępne są raporty generowane na żądanie zamawiającego z poziomu interfejsu GUI umożliwiające. - Raport bilingowy - Raport błędów	Wymagany

5. Wymagania pozafunkcjonalne

5.1 Wymagania w zakresie architektury

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany	
		On-Prem	SaaS
WA.01	System musi być zbudowany w architekturze mikroservisowej, która umożliwia niezależne wdrażanie, skalowanie i rozwijanie poszczególnych komponentów funkcjonalnych. Zastosowane przez Wykonawcę technologie muszą być zgodne ze stosem technologicznym Zamawiającego. W przypadku zaproponowania innej technologii Wykonawca zobowiązany jest zapewnić transfer wiedzy oraz dostarczyć odpowiednie licencje. Wprowadzenie przez Wykonawcę technologii spoza stosu technologicznego Zamawiającego, która spowoduje powstanie długu technologicznego, zobowiązuje Wykonawcę do aktywnego udziału w procedurze obsługi tego długu. Wykaz technologii używanych przez Zamawiającego został określony w: Załącznik nr 5 Stos technologiczny (podpunkt 2).	Wymagany	Niewymagany
WA.02	Wykonawca musi zapewnić, że obrazy maszyn wirtualnych i mikroservisów będą przechowywane w rejestrze obrazów udostępnionym przez Zamawiającego w ramach jego infrastruktury.	Wymagany	Niewymagany
WA.03	Wykonawca musi zapewnić, że Kod Źródłowy dostarczanego Systemu będzie	Wymagany	Niewymagany

	przechowywany na infrastrukturze Zamawiającego z kontrolą wersji Git.		
WA.04	Zastosowane przez Wykonawcę bazy danych muszą być zgodne ze stosem technologicznym Zamawiającego. W przypadku zaproponowania innej technologii Wykonawca zobowiązany jest zapewnić transfer wiedzy oraz dostarczyć odpowiednie licencje. Wprowadzenie przez Wykonawcę technologii spoza stosu technologicznego Zamawiającego, która spowoduje powstanie długu technologicznego, zobowiązuje Wykonawcę do aktywnego udziału w procedurze obsługi tego długu. Wykaz technologii używanych przez Zamawiającego w zakresie baz danych został określony w: Załącznik nr 5 Stos technologiczny (podpunkt 4).	Wymagany	Niewymagany
WA.05	System musi być zaprojektowany i wdrożony w środowisku klastrowym, zapewniającym wysoką dostępność oraz dynamiczne i automatyczne skalowanie zasobów obliczeniowych i bazodanowych.	Opcjonalny	Niewymagany
WA.06	Architektura mikroserwisowa musi zapewniać, że awaria instancji pojedynczego, niezależnego mikroserwisu nie powoduje niedostępności całego Systemu.	Wymagany	Niewymagany
WA.07	Architektura Systemu musi umożliwiać horyzontalne i wertykalne skalowanie komponentów.	Wymagany	Niewymagany
WA.08	System musi zapewniać możliwość aktualizacji bez przerywania działania pracy całego Systemu w zakresie aktualizacji typu „minor” i niższych.	Wymagany	Niewymagany
WA.09	System musi zapewniać środowiska: • DEV – deweloperskie, • TEST – testowe, • INT – integracyjno-szkoleniowe, • PRE-PROD – przedprodukcyjne, • PROD – produkcyjne. W przypadku dostarczania w modelu SaaS istnieje możliwość dostarczania środowiska produkcyjnego i jednego środowiska dla środowisk niższych.	Wymagany	Wymagany
WA.10	Architektura Systemu musi zapewnić zdolność do automatycznej naprawy (Auto-recovery):	Wymagany	Niewymagany

	- Architektura Systemu musi być wyposażona w wewnętrzny mechanizm nadzorczy, który automatycznie wykrywa i restartuje elementy infrastruktury oraz usługi Systemu, które przestały funkcjonować prawidłowo. - Mechanizm auto-recovery powinien minimalizować czas przestoju usług i zapewniać szybkie przywrócenie pełnej funkcjonalności Systemu.		
WA.11	Architektura Systemu musi zapewnić odporność na awarie (fault tolerance): - Architektura Systemu musi być odporna na awarie pojedynczych komponentów lub węzłów, zapewniając automatyczne przełączanie na sprawne zasoby bez utraty danych i bez zakłóceń w świadczeniu usług. W oparciu o mechanizmy takie jak load balancing, circuit breaking i retries. - Bazy danych muszą mieć formę klastrów typu active-active, lub hot-standby.	Wymagany	Niewymagany

5.2 Obsługiwane formaty danych i protokoły komunikacyjne

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany
WK.01	System musi udostępniać interfejsy REST API	Wymagany
WK.02	Dostęp do API musi być zabezpieczony z wykorzystaniem co najmniej jednego z poniższych mechanizmów (dopuszcza się zastosowanie obu jednocześnie): - uwierzytelniania opartego na certyfikacie klienta z wykorzystaniem protokołu TLS w wersji 1.3 lub wyższej, - klucza API (API Key) z obsługą rotacji kluczy.	Wymagany

5.3 Bezpieczeństwo i kontrola danych

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany On-prem	SaaS
WB.01	W momencie zgłoszenia przez Wykonawcę gotowości do testów penetracyjnych. System nie może zawierać potwierdzonych podatności ujawnionych w bazie programu CVE™, który kataloguje publicznie ujawnione podatności cyberbezpieczeństwa. (zgodnie z wydaniem obowiązującym na dzień zgłoszenia). Brak podatności musi być potwierdzony raportem z testów wykonanych przez niezależny podmiot na koszt Wykonawcy. Zamawiający zastrzega sobie prawo weryfikacji poziomu bezpieczeństwa na własny koszt.	Wymagany	Wymagany
WB.02	System nie może zawierać podatności sklasyfikowanych jako L1 OWASP ASVS v5 . Brak podatności musi być potwierdzony raportem z testów penetracyjnych wykonanych przez Zamawiającego.	Wymagany	Wymagany
WB.04	System musi wykorzystywać mechanizmy uwierzytelniania użytkowników wewnętrznych (system Active Directory Zamawiającego) zapewnione przez Zamawiającego w ramach dostępu do narzędzi administracyjnych Systemu.	Wymagany	Niewymagany
WB.05	Dostęp do funkcji Systemu musi być kontrolowany na podstawie ról i uprawnień.	Wymagany	Wymagany
WB.06	Przed Wdrożeniem Systemu Wykonawca opracuje model zagrożeń zgodny z metodyką PASTA lub STRIDE, na tej podstawie zaproponuje zmiany ograniczające zagrożenia do poziomu Niski. Sposób oceny podatności powinien być zgodny z CVSS Common Vulnerability Scoring System.	Wymagany	Wymagany
WB.07	Przed wdrożeniem Systemu Wykonawca przedstawi Software Bill of Material w jednym z formatów SPDX, CycloneDX lub SWID, wraz z określeniem podatności użytych komponentów w zakresie podatności technicznych i kwestii prawnych związanych z licencjami.	Wymagany	Wymagany

WB.08	Komponenty, zawarte w Software Bill of Material, które zostały użyte do opracowania Systemu na dzień odbioru Systemu nie mogą posiadać znanych podatności na poziomie wyższym niż Niski. Sposób oceny podatności powinien być zgodny z CVSS Common Vulnerability Scoring System.	Wymagany	Wymagany
WB.09	Sposób realizacji zadań oraz zabezpieczenia dostarczonych Systemów muszą spełniać wymagania opisane w: Załącznik nr 7 Polityka Bezpieczeństwa Informacji dla wykonawców.	Wymagany	Wymagany
WB.10	Zarządzanie wszystkimi danymi do uwierzytelnienia (a w szczególności dostępów do baz danych, interfejsów API) – tzw. „Secrety” - musi być zrealizowane w oparciu o system HashiCorp Vault dostarczony przez Zamawiającego.	Wymagany	Niewymagany
WB.11	Wykonawca przed zgłoszeniem gotowości do testów przeprowadzanych przez Zamawiającego przetestuje System zgodnie z procedurami opisanymi w dokumentach: OWASP Web Security Testing Guide i OWASP Application Security Verification Standard (ASVS) poziom L1 oraz dostarczy wynik tych testów.	Wymagany	Wymagany
WB.12	System logowania Systemu musi umożliwiać jego integrację z rozwiązaniem klasy SIEM. Oprogramowanie musi zapewniać wgląd w logi tylko dla Administratora	Wymagany	Niewymagany
WB.13	Logi audytu mają być dostępne do przetwarzania przez rozwiązanie monitoringu klasy SIEM. Mechanizmy logowania i logi muszą być chronione przed nadużyciem, takim jak manipulowanie, nieautoryzowany dostęp, modyfikacja i usuwanie po zapisaniu.	Wymagany	Wymagany
WB.14	System musi umożliwiać definiowanie poziomów szczegółowości logowania. Wymagana jest zgodność z OpenTelemetry.	Wymagany	Niewymagany
WB.15	Wykonawca dostarczy i przetestuje procedurę odtwarzania Systemu po awarii rozległej (katastrofie) z użyciem skryptów Infrastructure as Code (IaC). <u>działająca w sposób zautomatyzowany.</u>	Wymagany	Niewymagany
WB.16	System musi zapewniać szyfrowanie transmisji danych we wszystkich kanałach	Wymagany	Wymagany

	komunikacyjnych oraz we wszystkich integracjach. Wymaga się zastosowania następujących mechanizmów: • TLS w wersji 1.3 lub wyższej dla wszystkich połączeń HTTPS, • szyfrowanej komunikacji między aplikacją a serwerem bazodanowym (np. TLS lub inny protokół szyfrujący wspierany przez silnik bazy danych).		
WB.17	System musi być zabezpieczony przed atakami typu DoS (Denial of Service), w szczególności w przypadku, gdy atak jest inicjowany z poziomu uprawnionego punktu dostępu posiadającego prawidłową autoryzację. Zabezpieczenia muszą zapewniać ciągłość działania, odporność na przeciążenia oraz możliwość wykrywania i reagowania na anomalie w żądaniach.	Wymagany	Wymagany
WB.18	Wykonawca nie wykorzystuje danych przekazywanych do analizy w celach innych niż realizacja żądania	Wymagany	Wymagany
WB.19	Opisy interakcji lekowych wykorzystywane przez oferowany System muszą pochodzić z wiarygodnych udokumentowanych i aktualizowanych źródeł wiedzy medycznej. Kryteria: 1. Źródło eksperckie: Baza tworzona i utrzymywana przez zespół ekspertów z zakresu farmakologii klinicznej, farmacji, medycyny, z udokumentowanym procesem redakcyjnym i walidacyjnym. 2. Podstawa naukowa: Opisy interakcji muszą być oparte co najmniej na jednym z: • Publikacjach recenzowanych (peer-reviewed) • Charakterystykach produktów leczniczych • Wytocznych uznanych instytucji regulacyjnych (np. EMA, FDA) • Uznanych kompendiach farmakologicznych	Wymagany	Wymagany

--	--	--	--

5.4 Wymagania w zakresie wydajności i skalowalności

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany	
		On-Prem	SaaS
WW.01	System musi rejestrować czas rozpoczęcia, zakończenia oraz całkowity czas wykonywania operacji.	Wymagany	Wymagany
WW.02	System musi być skalowalny poziomo (horizontal scalability) w sposób umożliwiający zwiększenie wolumenu jednoczesnych sesji/transakcji użytkownika do poziomu 150% normatywnego obciążenia. Szczegółowe wymagania wydajnościowe znajdują się w: Załącznik nr 1 Usługa Serwisowa.	Wymagany	Niewymagany
WW.03	Wymagana jest możliwość integracji Systemu z systemami monitorowania Zamawiającego: • zasobów bazodanowych (np. repliki odczytu, alertowanie konieczności zwiększania pojemności dyskowej), • komponentów aplikacyjnych, • system wykrywania incydentów klasy SIEM.	Wymagany	Niewymagany
WW.04	Proces autoskalowania musi być transparentny dla użytkowników końcowych i nie wpływać na jakość świadczonych usług.	Wymagany	Wymagany

5.5 Wymagania w zakresie infrastruktury

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany	
		On-prem	SaaS
WI.01	System musi wykorzystywać infrastrukturę backupową Zamawiającego. Zastosowane przez Wykonawcę technologie w zakresie kopii zapasowych muszą być	Wymagany	Niewymagany

	zgodne ze stosem technologicznym Zamawiającego. W przypadku zaproponowania innej technologii Wykonawca zobowiązany jest zapewnić transfer wiedzy oraz udzielić lub zapewnić odpowiednie licencje. Wprowadzenie przez Wykonawcę technologii spoza stosu technologicznego Zamawiającego, która spowoduje powstanie długu technologicznego, zobowiązuje Wykonawcę do aktywnego udziału w procedurze obsługi tego długu. Wykaz technologii używanych przez Zamawiającego został określony w: Załącznik nr 5 Stos technologiczny (podpunkt 7).		
WI.02	System musi zapewnić mechanizmy umożliwiające tworzenie przyrostowych kopii zapasowych.	Wymagany	Niewymagany
WI.03	System musi umożliwiać przywrócenie stanu konfiguracji oraz danych operacyjnych na podstawie ostatnio wykonanych kopii zapasowych.	Wymagany	Niewymagany
WI.04	System musi mieć możliwość uruchomienia w drugim centrum przetwarzania danych, znajdującym się w innej lokalizacji. Czas przełączenia pomiędzy centrami przetwarzania danych zdefiniowany jest w: Załącznik nr 1 Usługa Serwisowa.	Wymagany	Niewymagany
WI.05	Wykonawca musi dostarczyć mechanizmy zarządzania tożsamością i uprawnieniami (IAM) umożliwiające integrację z centralnym repozytorium tożsamości użytkowników Zamawiającego (np. Active Directory lub równoważnym), z wykorzystaniem powszechnie stosowanych standardów branżowych (w szczególności LDAP/LDAPS, SAML 2.0 lub OpenID Connect). Mechanizm musi zapewniać centralne uwierzytelnianie i nadawanie uprawnień (role/attributy/grupy) oraz nie może opierać się wyłącznie na ręcznie utrzymywanych plikach lub lokalnych listach użytkowników jako jedynym mechanizmie zarządzania uprawnieniami.	Wymagany	Niewymagany

5.6 Wymagania dotyczące licencji i praw autorskich

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany
WL.01	Wykonawca udziela CeZ nieograniczonej czasowo, niewyłącznej, ograniczonej do terytorium RP licencji na korzystanie z Systemu (z wyłączeniem elementów Systemu stanowiących Rezultaty Dedykowane) oraz pozostałych Rezultatów Licencjonowanych, prawem do udzielania sublicencji. Ponadto, Wykonawca przenosi na CeZ autorskie prawa majątkowe do Rezultatów Dedykowanych, w zakresie określonym w Umowie. Wskazana powyżej licencja (lub przeniesienie autorskich praw majątkowych, jeśli takie przeniesienie nastąpi) musi obejmować prawo do wykonywania praw zależnych oraz do zezwalania na wykonywanie praw zależnych do Systemu oraz wyżej wymienionych Rezultatów. W celu umożliwienia Zamawiającemu wykonywania praw zależnych oraz udzielania zezwoleń na wykonywanie praw zależnych, zgodnie z poprzednim zdaniem, Wykonawca zobowiązuje się do przekazania Zamawiającemu, bez dodatkowych opłat, Rezultatów stanowiących program komputerowy w rozumieniu Prawa Autorskiego w postaci Kodu Źródłowego, na warunkach określonych w Umowie. Szczegółowy zakres i warunki udzielenia licencji oraz przeniesienia autorskich praw majątkowych określa Umowa.	Wymagany
WL.02	W przypadku wykorzystania przez Wykonawcę komponentów stron trzecich (w tym open source), Wykonawca jest zobowiązany do dostarczania pełnej listy użytych komponentów (SBOM – Software Bill of Materials) wraz z ich nazwami, wersjami, licencjami. Zamawiający nie dopuszcza wykorzystania oprogramowania objętego licencjami „wirusowymi” (np. GPL, AGPL), które mogłyby powodować obowiązek ujawnienia Kodu Źródłowego całości rozwiązania.	Wymagany
WL.03	Wykonawca zapewnia wsparcie do wszystkich komponentów Systemu oraz ich aktualizacje.	Wymagany

5.7 Wymagania w zakresie użyteczności

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany
---------------	----------------	--------------------------------

20 z 34

WU.01	System musi posiadać interfejsy użytkownika zgodne z WCAG 2.1 na poziomie A i AA. Zgodność ta musi być zapewniona przez Wykonawcę na etapie odbioru Systemu.	Wymagany
WU.02	Komunikaty błędów muszą być czytelne i nie mogą zawierać szczegółów technicznych (np. stack trace).	Wymagany
WU.03	Wszystkie interfejsy użytkownika muszą być dostępne w języku polskim.	Wymagany
WU.04	Dokumentacja rozwiązania musi być zgodna z zapisami zawartymi w rozdziale „Wymagania dotyczące Dokumentacji”.	Wymagany

5.8 Wymagania dotyczące Dokumentacji

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany	
		On-prem	SaaS
WD.01	Wykonawca musi przekazać dokumentację Systemu w oparciu o wymagania zawarte w dokumencie: Załącznik nr 2 Wymagania dla Dokumentacji	Wymagany	Niewymagany

5.9 Rejestrowanie zdarzeń i logi Systemowe

Kod wymagania	Opis wymagania	Parametr wymagany / punktowany
WZ.01	System musi rejestrować wszystkie operacje Systemowe i użytkowe w dzienniku zdarzeń, w tym: • zdarzenia administracyjne, • zmiany konfiguracji, • błędy przetwarzania, • zmiany w ustawieniach użytkowników.	Wymagany
WZ.02	Wykonawca musi zapewnić dostęp i przeglądanie logów oraz dziennika zdarzeń w aplikacji Grafana, która znajduje się w stosie technologicznym Zamawiającego.	Wymagane
WZ.03	System musi dla każdego wpisu w dzienniku zdarzeń zapisywać co najmniej: • Uuid żądania • identyfikator użytkownika, • czas operacji,	Wymagany

	• typ operacji, • identyfikator obiektu • rezultat (sukces, błąd).	
WZ.04	System musi rejestrować każde użycie interfejsów API zewnętrznych, w tym co najmniej: • żądanie, • nadawca, • kod odpowiedzi, • czas realizacji.	Wymagany
WZ.05	System musi umożliwiać generowanie powiadomień w przypadku wystąpienia określonych zdarzeń zdefiniowanych przez Zamawiającego.	Wymagany
WZ.06	System musi umożliwiać rejestrowanie operacji użytkowników (logi audytowe), w tym: • logowania, • uruchamiania procesów, • edycji konfiguracji, • zmian uprawnień.	Wymagany
WZ.07	Logi audytowe muszą być dostępne dla administratorów i możliwe do eksportu lub integracji z zewnętrznymi systemami SIEM (Security Information and Event Management). Zastosowane przez Wykonawcę technologie w zakresie logów audytowych muszą być zgodne ze stosem technologicznym Zamawiającego. W przypadku zaproponowania innej technologii Wykonawca zobowiązany jest zapewnić transfer wiedzy oraz dostarczyć odpowiednie licencje. Wprowadzenie przez Wykonawcę technologii spoza stosu technologicznego Zamawiającego, która spowoduje powstanie długu technologicznego, zobowiązuje Wykonawcę do aktywnego udziału w procedurze obsługi tego długu. Wykaz technologii używanych przez Zamawiającego został określony w: Załącznik nr 5 Stos technologiczny (podpunkt 9).	Wymagany
WZ.08	System musi umożliwiać konfigurację poziomu szczegółowości logowania operacji (np. tylko błędy, wszystkie działania administracyjne).	Wymagany

6. Dostarczane elementy

6.1 System

Wykonawca dostarczy najnowszą, stabilną wersję gotowego Systemu, który realizuje wymagania funkcjonalne i pozafunkcjonalne określone w niniejszym OPZ.

Wymagania dotyczące formy dostarczenia Systemu zależą od wybranego przez Zamawiającego modelu świadczenia usługi, określonego w pkt 6.2

6.2 Model świadczenia usługi

Zamawiający dopuszcza jeden z dwóch modeli świadczenia usługi:

1. Model w infrastrukturze Zamawiającego (on-prem) z licencją na okres 60 miesięcy, w ramach którego Wykonawca dostarczy System w architekturze skonteneryzowanej, gotowej do implementacji w środowisku wskazanym przez Zamawiającego wraz z gotowymi do uruchomienia pakietami instalacyjnymi wraz ze wszystkimi niezbędnymi bibliotekami, zależnościami, skryptami, modelami logicznymi i dokumentacją w języku polskim, a także zapewni wsparcie techniczne na etapie instalacji, wdrożenia i stabilizacji. Zamawiający wymaga od Wykonawcy dostarczenia precyzyjnej specyfikacji wymagań infrastrukturalnych (minimalnych i rekomendowanych) oraz opracowania instrukcji wdrożenia w środowisku Kubernetes z wykorzystaniem procesów CI/CD.
2. Model SaaS (Software as a Service) na okres 60 miesięcy, rozliczany na podstawie liczby wywołań - interakcji Użytkowników z Systemem w miesięcznym okresie rozliczeniowym, z możliwością zastosowania alternatywnego wariantu rozliczenia w formie stałej, ryczałtowej opłaty miesięcznej obejmującej nielimitowaną liczbę wywołań. System będzie utrzymywany w infrastrukturze Wykonawcy zlokalizowanej zgodnie z polskimi i europejskimi przepisami dotyczącymi przetwarzania danych i powinna zapewniać spełnienie wymagań odpowiadających co najmniej poziomowi SCCO2, w zakresie adekwatnym do przetwarzania danych medycznych oraz integracji z systemami ochrony zdrowia sektora publicznego. Wymagania dotyczące konteneryzacji i instrukcji wdrożeniowych nie mają zastosowania.

Wykonawca może złożyć ofertę na jeden lub oba modele świadczenia usługi. W przypadku złożenia oferty na oba modele, cena musi zostać wskazana odrębnie dla każdego modelu. Zamawiający dokona wyboru jednego modelu realizacji zamówienia na podstawie kryteriów oceny ofert.

W przypadku modelu instalowanego w infrastrukturze Zamawiającego w zakresie wymaganej infrastruktury technicznej wymagane jest dostarczenie precyzyjnej specyfikacji wymagań

minimalnych oraz rekomendowanych, odnoszących się do wskazanej liczby zapytań od Użytkowników korzystających z systemu. Przedstawiony model powinien uwzględniać wymagania Zamawiającego co do dostępnej infrastruktury oraz stosu technologicznego zgodnie z opisem w wymaganiach.

W przypadku dostarczenia Systemu w modelu SaaS rozliczenie będzie dokonywane na podstawie liczby wywołań API w miesięcznym okresie rozliczeniowym. Wykonawca przedstawi ofertę cenową w podziale na przedziały wolumenowe wywołań w układzie miesięcznym. Dopuszcza się jednocześnie możliwość zaoferowania stałej, ryczałtowej opłaty miesięcznej obejmującej nielimitowaną liczbę wywołań. Rozliczenie może uwzględniać dodatkowe parametry, takie jak liczba leków, liczba par lekowych oraz liczba wygenerowanych alertów, o ile mają one wpływ na rzeczywiste obciążenie Systemu.

6.3 Licencje i Kod Źródłowy

Wykonawca udzieli Zamawiającemu licencji na korzystanie z Systemu.

Licencja musi co najmniej zapewniać:

- Przekazanie Kodów Źródłowych oraz dokumentacji technicznej w sytuacji instalacji na infrastrukturze zamawiającego,
- Ograniczenia lub ich brak w zakresie ilościowych oraz czasowych dotyczących liczby realizowanych operacji, przetwarzanych danych oraz wywołań interfejsów API w ramach eksploatacji rozwiązania przez Zamawiającego zgodnie z oferowanym modelem dostawy,

6.4 Usługa Serwisowa

Wykonawca zobowiązany jest do świadczenia Usług Serwisowych przez okres i na warunkach określonych w Umowie i Załączniku nr 1 Usługa Serwisowa.

Opis i zakres Usługi Serwisowej są określone w Załączniku nr 1 Usługa Serwisowa.

6.5 Gwarancja

Wykonawca udzieli Zamawiającemu Gwarancji na System i poszczególne Rezultaty na zasadach określonych w Umowie.

6.6 Instruktaż stanowiskowy

Na moment odbioru Systemu, Wykonawca musi dostarczyć kompleksowe materiały instruktażowe i dokumentację techniczną oraz przeprowadzić instruktaże dla personelu IT max. 16 osób.

Wykonawca musi zapewnić:

- Materiały instruktażowe, umożliwiające samodzielne zapoznanie się z obsługą i konfiguracją Systemu.
- Aktualizację materiałów instruktażowych przy każdej istotniej zmianie Systemu lub sposobu jej obsługi,

Przygotowanie materiałów instruktażowych:

Zakres zobowiązań Wykonawcy:

- Wykonawca opracuje i uzgodni z Zamawiającym zakres merytoryczny materiałów instruktażowych (forma, szczegółowy zakres materiałów). Zawartość merytoryczna materiałów instruktażowych, po zapoznaniu się z ich treścią, musi umożliwiać samodzielną pracę z Systemem,
- Wykonawca opracuje i przedstawi do akceptacji Zamawiającego konspekt materiałów instruktażowych związanych z Systemem. Konspekt musi zawierać podział na moduły tematyczne. Wykonawca przystąpi do przygotowania instruktaży stanowiskowych, po akceptacji konspektu przez Zamawiającego.
- Wykonawca przygotuje i opracuje materiały instruktażowe (poradniki/przewodniki/instruktaże multimedialne) zawierające m.in. opis oraz sposób korzystania z Systemu.
- Wykonawca w ramach przygotowywania materiałów dla instruktaży stanowiskowych opracuje co najmniej:
 - o przewodnik/instrukcję korzystania z poszczególnych funkcjonalności Systemu,
 - o materiały uzupełniające (filmy instruktażowe, animacje, publikacje itp.).
- Materiały instruktażowe muszą być możliwe do opublikowania na stronach informacyjnych Zamawiającego.
- Materiały instruktażowe muszą być dodatkowo opracowane w formie umożliwiającej wydruk i powielanie.
- Materiały instruktażowe dedykowane będą administratorom IT obsługującym System.

- Treści instruktaży musi być w języku polskim.
- Materiały w formie filmów instruktażowych muszą zawierać narrację głosową w języku polskim.
- Materiały instruktażowe muszą zakładać wykorzystanie przez użytkowników oprogramowania, które nie będzie wymagało ponoszenia żadnych dodatkowych kosztów z tego tytułu przez cały okres trwania Umowy.
- Instruktaż musi zawierać podział na moduły, lekcje, ekrany Instruktaż w zakresie obsługi Systemu powinien dotyczyć m.in. zasad wykorzystania Systemu oraz pokazywać w szczególności wszystkie jego funkcjonalności.
- Każdy materiał instruktażowy, będzie się składać z następujących części:
 - ✓ Spis treści (umożliwiający przejście do wybranej części oraz wybranego zagadnienia, np. poprzez hiperlinki);
 - ✓ Wprowadzenie do tematu konkretnego instruktażu, informacje podstawowe o przedmiocie kursu, zakresie tematyki kursu;
 - ✓ Część zasadnicza, czyli część teoretyczna, polegająca na przekazaniu wiedzy;
 - ✓ W ciągu 4 tygodni po podpisaniu umowy, Wykonawca przedstawi Zamawiającemu do akceptacji projekt graficzny instruktażu. Odbiór końcowy projektu graficznego nastąpi po spełnieniu następujących kryteriów akceptacji:
 - Zgodność z szatą graficzną projektu „e-Zdrowie KPO” (Załącznik nr 10 Księga Identyfikacji Wizualnej KPO),
 - Zrozumiałość i czytelność, projekt graficzny musi być czytelny i zrozumiały dla użytkownika,
 - Projekt szaty graficznej musi być dostarczony w wersji cyfrowej i drukowanej, z opcją dostosowania dla osób z niepełnosprawnościami (WCAG 2.1).
- Po otrzymaniu projektu szaty graficznej Zamawiający ma 5 dni roboczych na jego weryfikację pod kątem zgodności z kryteriami akceptacji. W przypadku stwierdzenia niezgodności z wymaganiami, Zamawiający prześle Wykonawcy listę uwag i koniecznych do wprowadzenia poprawek. Wykonawca jest zobowiązany do naniesienia wskazanych poprawek i przedstawienia zmodyfikowanego projektu w terminie nie dłuższym niż 5 dni roboczych od otrzymania uwag. Po ponownym złożeniu projektu, procedura weryfikacji rozpoczyna się od nowa.
- Materiały instruktażowe będą aktualizowane wraz z ewentualnymi zmianami w Systemie.
- Wykonawca będzie aktualizował materiały przez cały okres Gwarancji Systemu.

- Szata graficzna materiałów instruktażowych musi być spójna z szatą graficzną projektu „e-Zdrowie KPO” oraz zgodnie z wytycznymi Krajowego Planu Odbudowy i Zwiększania Odporności. Strategia promocji i informacji KPO jest dostępna w: Załącznik nr 10 Księga Identyfikacji Wizualnej KPO
- Materiały instruktażowe muszą zostać przygotowane w programie umożliwiającym Zamawiającemu ich późniejszą, samodzielną edycję. Wykonawca zobowiązany jest przekazać Zamawiającemu pliki projektowe instruktaży.
- Wykonawca zapewni opiekę techniczną instruktaży i od momentu ich uruchomienia do zakończenia trwania okresu Gwarancji.
- Obsługa instruktaży prowadzona będzie przez cały okres trwania Umowy.
- Wykonawca zobowiązany jest do przekazania Zamawiającemu plików z treściami instruktaży, wytworzonych w ramach Umowy (np. pliki z treściami dydaktycznymi, pliki multimedialne, teksty elektroniczne w formacie PDF, HTML) na etapie odbioru, oraz zapewniać aktualizacje aż do zakończenia okresu utrzymania Systemu.

7. Obowiązki Wykonawcy

7.1 Wersjonowanie Systemu i planowane przerwy serwisowe

System musi być wersjonowany zgodnie ze schematem major/minor.

Wykonawca zobowiązany jest do zapewnienia nieprzerwanego, stabilnego działania Systemu będącego przedmiotem zamówienia, przez cały okres trwania umowy, w modelu 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.

Przerwy serwisowe

- Planowane przerwy serwisowe (okresy niedostępności aplikacji) są dopuszczalne wyłącznie w przypadku wdrażania nowej wersji oprogramowania oznaczonej jako **major**, tj. zmiana pierwszego numeru w oznaczeniu wersji (np. z wersji 2.x.x na 3.0.0).
- O planowanej przerwie serwisowej Wykonawca jest zobowiązany poinformować Zamawiającego z wyprzedzeniem co najmniej 7 dni roboczych, przekazując szczegółowe informacje dotyczące:
 - terminu i planowanego czasu trwania przerwy,
 - zakresu planowanych prac,

- wpływu na dostępność Systemu.

Przerwa serwisowa nie może trwać dłużej niż 4 godziny, a łączny czas wszystkich planowanych przerw nie może przekroczyć 16 godzin w roku kalendarzowym.

W szczególnie uzasadnionych przypadkach np. tj.:

- konieczność instalacji oprogramowania na środowisku PROD przed zakończeniem wszystkich procedur testowych;
- problemy z funkcjonowaniem systemów Zamawiającego służących do świadczenia Usług przez Wykonawcę (np. systemy monitoringu, systemy obsługi zgłoszeń);
- problemy z funkcjonowaniem infrastruktury Zamawiającego mające wpływ na świadczenie Usług przez Wykonawcę

Zamawiający dopuszcza możliwość wydłużenia przerwy serwisowej na zasadach określonych poniżej:

- Wykonawca, w przypadku zaistnienia jednego z powyżej opisanych przypadków, zwraca się do Kierownika Projektu Zamawiającego z wnioskiem o wydłużenie przerwy serwisowej, wniosek wymaga zgody Zamawiającego, przy czym Zamawiający zobowiązuje się do niezwłocznego rozpoznania wniosku;
- Uruchomienie nowej wersji Systemu w środowisku produkcyjnym zostanie przeprowadzone przez Zamawiającego. Ostateczną decyzję o terminie uruchomienia nowej wersji Systemu podejmie każdorazowo Zamawiający. W zakresie wdrożenia produkcyjnego Wykonawca zobowiązany jest do zapewnienia wsparcia technicznego zgodnie z zapisami w: Załącznik nr 1 Usługa Serwisowa.

7.2 Testy wydajnościowe

Wykonawca Systemu będzie uczestniczył w testach wydajnościowych, których celem jest weryfikacja: czy System spełnia określone wymagania dotyczące szybkości działania, stabilności i skalowalności pod zdefiniowanym obciążeniem.

Celem będzie również identyfikacja i eliminacja "wąskich gardeł" wydajnościowych, które mogłyby negatywnie wpłynąć na doświadczenia użytkowników końcowych oraz zapewnienie, że System będzie w stanie obsłużyć przewidywany ruch w przyszłości. Weryfikacja będzie wykonywana na podstawie raportów z testów.

7.2.1 Rodzaje testów:

Poniżej opisane rodzaje testów zostaną przeprowadzone po zgłoszeniu gotowości przez Wykonawcę, na etapie Odbioru Systemu.

Wykonawca Systemu musi przygotować i przedstawić mailowo do akceptacji mailowej Zamawiającego szczegółowy plan / harmonogram testów wydajnościowych, który będzie zawierał co najmniej następujące elementy:

- **Testy obciążeniowe (Load Testing):** Symulacja oczekiwanego, normalnego obciążenia Systemu w celu weryfikacji, czy spełnia on podstawowe wymagania wydajnościowe. Scenariusze testowe będą odzwierciedlać typowe zachowania użytkowników.
- **Testy przeciążeniowe (Stress Testing):** Stopniowe zwiększanie obciążenia powyżej normalnego poziomu w celu zidentyfikowania punktu krytycznego Systemu.
- **Testy wytrzymałościowe (Soak/Endurance Testing):** Długotrwałe testy pod normalnym obciążeniem (np. 8, 12, 24 godziny) w celu wykrycia problemów, które ujawniają się po dłuższym czasie działania, takich jak wycieki pamięci, niestabilność połączeń z bazą danych itp.
- **Testy skokowe (Spike Testing):** Symulacja nagłych, gwałtownych wzrostów obciążenia w celu weryfikacji, jak System radzi sobie z nagłymi skokami ruchu (np. podczas napływu zleceń na badanie w piku: 8.00-10.00)
- Zamawiający ma możliwość weryfikacji zgodności merytorycznej zgodnie z wymaganiami zawartymi w dokumentacji przetargowej powołując zespół biegłych.
- Terminy i częstotliwość realizacji poszczególnych rodzajów testów.

7.2.2. Środowisko testowe

- Wykonawca odpowiada za dostarczenie danych testowych. Dane testowe powinny być zanonimizowane i odzwierciedlać wolumen i strukturę danych produkcyjnych.
- Narzędzia monitorujące powinny być skonfigurowane do zbierania metryk zarówno po stronie serwera (wykorzystanie zasobów), jak i po stronie aplikacji (czasy odpowiedzi, przepustowość). Wykonawca zobowiązany jest do zapewnienia integracji z oprogramowaniem monitorującym Zamawiającego (Zabbix, Grafana), w sposób umożliwiający gromadzenie i analizę danych w środowisku Zamawiającego. Zamawiający dopuszcza wykorzystanie przez Wykonawcę własnych narzędzi monitorujących, jednak wszystkie metryki muszą trafić do zasobów i oprogramowania monitorującego Zamawiającego (Zabbix, Grafana).

7.2.3. Cykliczność testów

Testy wydajnościowe będą przeprowadzane cyklicznie przez Zamawiającego, zgodnie z planem / harmonogramem:

- **Przed wdrożeniem nowej wersji Systemu (Release Testing):** Każde nowe, istotne wydanie oprogramowania powinno być poprzedzone pełnym cyklem testów wydajnościowych.
- **Po wprowadzeniu istotnych zmian w infrastrukturze:** Zmiany w konfiguracji serwerów, sieci, bazy danych itp. wymagają ponownego przeprowadzenia testów.
- **Okresowo co kwartał:** Regularne testy pozwalają na weryfikację utrzymania wydajności Systemu w czasie, szczególnie w kontekście rosnącej liczby użytkowników i danych.
- **Na żądanie:** W przypadku wystąpienia problemów z wydajnością na środowisku produkcyjnym, powinna istnieć możliwość przeprowadzenia testów ad-hoc w celu zdiagnozowania przyczyny.

7.3 Testy bezpieczeństwa

Wykonawca Systemu jest zobowiązany do zaprojektowania, zbudowania i dostarczenia Systemu, którego bezpieczeństwo zostanie zweryfikowane i będzie podlegało testom bezpieczeństwa podczas trwania umowy.

Wykonawca musi proaktywnie identyfikować i eliminować zagrożenia na etapie projektowym oraz reagować na wykryte podatności, usuwając je na własny koszt. Wykonawca jest zobowiązany do aktywnego uczestnictwa w zintegrowanych testach, organizowanych przez Zamawiającego.

Lista zadań i testów bezpieczeństwa, które muszą być zrealizowane przez Wykonawcę:

- **Modelowanie zagrożeń:** Przed wdrożeniem Wykonawca jest zobowiązany opracować model zagrożeń dla Systemu, stosując metodykę PASTA lub tożsamą. Na tej podstawie musi zaproponować zmiany w architekturze, które ograniczą zidentyfikowane zagrożenia do poziomu "Niski".
- **Analiza składu oprogramowania (SBOM):** Wykonawca musi przedstawić kompletną listę użytych komponentów i bibliotek (Software Bill of Materials). Na dzień odbioru Systemu, komponenty te nie mogą posiadać znanych podatności na poziomie wyższym niż "Niski".

- Testy penetracyjne: System, na dzień zgłoszenia przez Wykonawcę gotowości do testów, nie może zawierać podatności wymienionych w OWASP Top 10 oraz CWE Top 25. Testy penetracyjne zostaną wykonane przez Zamawiającego w terminie 15 dni roboczych od dnia zgłoszenia przez Wykonawcę gotowości, a zidentyfikowane podatności zostaną rozwiązane przez Wykonawcę. W przypadku zidentyfikowania jakichkolwiek podatności na poziomie „Krytyczny”, „Wysoki” lub „Średni”, Wykonawca jest zobowiązany do ich usunięcia, a procedura zostanie powtórzona do momentu uzyskania podatności maksymalnie na poziomie „Niski”.
- Testy zgodności z polityką CeZ: Wykonawca musi przetestować System zgodnie ze sposobem opisanym w Załączniku nr 7 Polityka bezpieczeństwa CeZ dla wykonawców. Wszystkie podatności o poziomie średnim i wyższym, wykryte podczas tych testów, muszą zostać usunięte na koszt Wykonawcy, a testy powtórzone.
- Testowanie Procedur Odtwarzania po Awarii (Disaster Recovery): Wykonawca ma obowiązek dostarczyć i przetestować procedurę odtwarzania Systemu po rozległej awarii (katastrofie) z wykorzystaniem skryptów Infrastructure as Code (IaC).
- Dostarczenie Dokumentacji dla DPIA: Wykonawca musi dostarczyć Zamawiającemu wszelkie informacje o Systemie, które są niezbędne do przeprowadzenia i aktualizacji DPIA zgodnie z art. 35 RODO.

7.4 Testy integracyjne

Testy integracyjne zostaną przeprowadzone na etapie odbioru Systemu.

Wykonawca jest zobowiązany do aktywnego udziału we wspólnych, zintegrowanych testach End-To-End (E2E) organizowanych przez Zamawiającego.

Celem testów E2E jest weryfikacja kompletnego przepływu zapytań w ramach ekosystemu Pe-profil – od jego przyjęcia przez System, przez przekazanie do Systemu, aż po odbiór wyniku i udostępnienie go przez interfejs Zamawiającego.

W ramach testów weryfikowana będzie między innymi integralność danych, a więc potwierdzenie, że wynik udostępniany przez System jest tożsamy z wynikiem wygenerowanym przez System.

7.5 Weryfikacja jakości Kodu Źródłowego

W przypadku modelu instalowanego na infrastrukturze zamawiającego wykonawca zobowiązany jest do dostarczenia Zamawiającemu Kodu Źródłowego wraz z dokumentacją techniczną, zgodnego z wymaganiami jakościowymi określonymi w Załączniku nr 6 Wymagania jakościowe Kodu Źródłowego.

Dostarczony Kod Źródłowy podlega weryfikacji przez Zamawiającego przy użyciu narzędzia SonarQube lub równoważnego, zgodnie z procedurą opisaną w ww. Załączniku.

Weryfikacja jakości Kodu Źródłowego stanowi integralny element odbioru dostarczanego Systemu. Do momentu spełnienia wszystkich kryteriów jakościowych na poziomie określonym przez Zamawiającego, odbiór Systemu nie nastąpi.

W przypadku niespełnienia któregośkolwiek z kryteriów jakościowych, Wykonawca zobowiązany jest do usunięcia stwierdzonych niezgodności i ponownego przekazania Kodu Źródłowego do weryfikacji.

7.6 Usługi Gwarancyjne i Serwisowe

Usługa opisana w Załącznik nr 1 Usługa Serwisowa

7.7 Usługi Rozwojowe

Zamawiający wymaga zapewnienia Usług Rozwojowych w okresie obowiązywania Umowy w wymiarze godzin, w tym godzin w ramach zamówienia podstawowego, godzin w ramach zamówienia opcjonalnego.

Usługi Rozwojowe będą wykorzystywane do rozwoju i dostosowania Sytemu do zmieniających się w czasie potrzeb Zamawiającego. Zamawiający, chcąc zrealizować daną funkcjonalność będzie zlecał takie żądanie do Wykonawcy. Wykonawca dokona szacowania Pracochłonności (liczby Roboczogodzin) i terminu ich dostarczenia. Następnie Zamawiający po akceptacji szacowania zleci wykonanie prac.

7.8 Ogólny Harmonogram Wdrożenia Systemu

Przygotowanie szczegółowego harmonogramu wdrożenia jest obowiązkiem Wykonawcy i podlega akceptacji przez Zamawiającego.

7.9 Dokumentacja

7.9.1 Wymagania ogólne

1. Dokumentacja musi być sporządzona w języku polskim.

2. Każda Dokumentacja powstała w wyniku realizacji zamówienia i przekazana Zamawiającemu przez Wykonawcę stanowi własność Zamawiającego. Zamawiający ma prawo udostępniać Dokumentację osobom trzecim w sposób nienaruszający praw autorskich.
3. Wykonawca dostarczy szczegółową Dokumentację komponentów firm trzecich użytych w dostarczonym Systemie, w tym także dostarczaną przez ich producentów. Dokumentacja ta może występować w języku angielskim, jeśli nie ma tłumaczenia na język polski.
4. Dokumentacja musi gwarantować kompletność dokumentu rozumianą jako pełne, bez wyraźnych i ewidentnych braków, przedstawienie omawianego problemu obejmujące całość z danego rozpatrywanego zakresu zagadnienia.
5. Zawartość Dokumentacji musi być zgodna z wdrożonym rozwiązaniem.
6. Dokumentacja musi być aktualizowana o nowe zagadnienia, jeśli zostaną wprowadzone do Systemu w ramach Usług Gwarancyjnych i Serwisowych.

7.9.2 Dokumentacja Administratora Systemu

1. Dokumentacja Administratora Systemu musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych i awaryjnych.
2. Dokumentacja Administratora Systemu powinna być dostępna w postaci elektronicznej umożliwiającej przeszukiwanie oraz odnajdywanie konkretnych tematów.
3. Dokumentacja Administratora Systemu obejmować będzie, co najmniej:
 - 1) szczegółową (krok po kroku) instrukcję instalacji i konfiguracji Systemu,
 - 2) opis parametrów instalacyjnych i konfiguracyjnych wraz z opisem dopuszczalnych wartości i ich wpływem na działanie rozwiązania,
 - 3) szczegółową (krok po kroku) instrukcję wgrywania nowych wersji systemu,
 - 4) szczegółowy opis możliwych do zastosowania ról i uprawnień wraz z ich wpływem na działania rozwiązania.

7.9.3 Dokumentacja Użytkownika Systemu

1. Wykonawca dostarczy Dokumentację użytkownika oraz opis ścieżek postępowania (jak wykonać daną czynność w aplikacji).
2. Dokumentacja Użytkownika Systemu powinna być dostępna w postaci elektronicznej umożliwiającej przeszukiwanie oraz odnajdywanie konkretnych tematów.
3. Dokumentacja użytkownika musi zawierać opis pełnej funkcjonalności Systemu w sposób przejrzysty umożliwiający samodzielne użytkowanie Systemu.
4. Dokumentacja musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych.
5. Wykonawca dostarczy szczegółową Dokumentację komponentów firm trzecich użytych w dostarczonym Systemie, w tym także dostarczaną przez ich producentów

6. Zamawiający wymaga od Wykonawcy przekazania przed podpisaniem Protokołu Odbioru Końcowego:
7. 2 egzemplarzy aktualnej dokumentacji administratora w języku polskim w postaci papierowej,
8. 2 egzemplarzy aktualnej dokumentacji użytkownika w języku polskim w postaci papierowej,
9. 2 zestawów egzemplarzy dokumentacji administratora i użytkownika w postaci elektronicznej, na niezależnych nośnikach w tym na jednym z aktywną blokadą zapisu i jednym umożliwiającym Zamawiającemu wprowadzanie do niej korekt, zmian i uzupełnień.